

PCT

REQUETE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire (facultatif)
(12 caractères au maximum) PCT 3630/BC

Cadre n° I TITRE DE L'INVENTION
Microprocesseur ou microcalculateur imprévisible.

Cadre n° II DEPOSANT

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

BULL CP8
68, route de Versailles
BP 45
78430 LOUVECIENNES
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone

(33) 1 39.66.61.76

n° de télécopieur

(33) 1 39.66.61.73

n° de téléimprimeur

Nationalité (nom de l'Etat) :

FRANCE

Domicile (nom de l'Etat) :

FRANCE

Cette personne est déposant pour :

☐ tous les Etats désignés

☒ tous les Etats désignés sauf les Etats-Unis d'Amérique

☐ les Etats-Unis d'Amérique seulement

☐ les Etats indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DEPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

UGON Michel
06 Rue des Cépages
78310 MAUREPAS
FRANCE

Cette personne est :

☐ déposant seulement

☒ déposant et inventeur

☐ inventeur seulement
(Si cette case est cochée, ne pas remplir la suite.)

Nationalité (nom de l'Etat) :

FRANCE

Domicile (nom de l'Etat) :

FRANCE

Cette personne est déposant pour :

☐ tous les Etats désignés

☐ tous les Etats désignés sauf les Etats-Unis d'Amérique

☒ les Etats-Unis d'Amérique seulement

☐ les Etats indiqués dans le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRESENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme :

☒ mandataire

☐ représentant commun

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)

BULL S.A
CORLU Bernard
PC59C18 / 68, route de Versailles
78434 LOUVECIENNES Cédex (FRANCE)

n° de téléphone

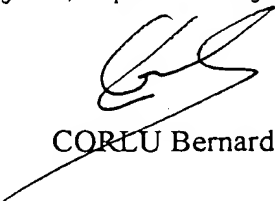
(33) 1 39.66.61.76

n° de télécopieur

(33) 1 39.66.61.73

n° de téléimprimeur

☐ Cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

Cadre n° VI REVENDEICATION DE PRIORITE			D'autres revendications de priorité sont indiquées dans le cadre supplémentaire <input type="checkbox"/>
La priorité de la ou des demandes antérieures suivantes est revendiquée :			
Pays <i>(dans lequel ou pour lequel la demande a été déposée)</i>	Date de dépôt <i>(jour/mois/année)</i>	Demande n°	Office de dépôt <i>(seulement s'il s'agit d'une demande régionale ou internationale)</i>
(1) FRANCE	26 juin 1997 (26.06.97)	97 07995	
(2)			
(3)			
<p><i>Cocher la case ci-dessous si la copie certifiée conforme de la demande antérieure doit être délivrée par l'office qui, aux fins de la présente demande internationale, est l'office récepteur (une taxe peut être exigée) :</i></p> <p><input checked="" type="checkbox"/> L'office récepteur est prié de préparer, et de transmettre au Bureau international, une copie certifiée conforme de la ou des demandes antérieures indiquées ci-dessus au(x) point(s) : <u>1</u></p>			
Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE			
<p>Choix de l'administration chargée de la recherche internationale (ISA) <i>(Si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) :</i> ISA / _____</p> <p>Recherche antérieure Remplir si une recherche (internationale, de type international ou autre) a déjà été effectuée par l'administration chargée de la recherche internationale ou demandée à cette administration et si cette administration est maintenant priée de fonder la recherche internationale, dans la mesure du possible, sur les résultats de cette recherche antérieure. Pour permettre d'identifier cette recherche ou cette demande de recherche, donner les renseignements demandés ci-après pour la demande de brevet pertinente (ou sa traduction) ou pour la demande de recherche :</p> <p>Pays (ou office régional) : FRANCE Date (jour/mois/année) : 26 juin 1997 (26.06.97) Numéro : 97 07995</p>			
Cadre n° VIII BORDEREAU			
<p>La présente demande internationale comprend le nombre de feuilles suivant :</p> <p>1. requête : 03 feuilles 2. description : 19 feuilles 3. revendications : 04 feuilles 4. abrégé : 01 feuilles 5. dessins : 03 feuilles Total : 30 feuilles</p>		<p>Le ou les éléments cochés ci-après sont joints à la présente demande internationale :</p> <p>1. <input checked="" type="checkbox"/> pouvoir distinct signé 5. <input type="checkbox"/> feuille de calcul des taxes 2. <input type="checkbox"/> copie du pouvoir général 6. <input type="checkbox"/> indications séparées concernant des micro-organismes déposés 3. <input type="checkbox"/> explication de l'absence d'une signature 7. <input type="checkbox"/> listage de séquence de nucléotides ou d'acides aminés (disquette) 4. <input type="checkbox"/> document(s) de priorité (indiqué(s) dans le cadre n° VI au(x) point(s)) : 8. <input checked="" type="checkbox"/> autres éléments (préciser) : Rapport de Recherche</p>	
La figure n° <u>01</u> des dessins (le cas échéant) est proposée pour publication avec l'abrégé.			
Cadre n° IX SIGNATURE DU DEPOSANT OU DU MANDATAIRE			
A côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.			
 CORLU Bernard (mandataire)			

Réservé à l'office récepteur	
1. Date effective de réception des pièces supposées constituer la demande internationale :	2. Dessins : <input type="checkbox"/> reçus : <input type="checkbox"/> non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :	
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :	
5. Administration chargée de la recherche internationale indiquée par le déposant : ISA /	6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche

Réservé au Bureau international
Date de réception de l'exemplaire original par le Bureau international :

Cadre n° V DESIGNATION D'ETATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) (cocher les cases appropriées; une au moins doit l'être):

Brevet régional

- ☐ AP Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, SD Soudan, SZ Swaziland, UG Ouganda, ZW Zimbabwe et tout autre Etat qui est un Etat contractant du Protocole de Harare et du PCT
- ☐ EA Brevet eurasién : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre Etat qui est un Etat contractant de la Convention sur le brevet eurasién et du PCT
- ☒ EP Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre Etat qui est un Etat contractant de la Convention sur le brevet européen et du PCT
- ☐ OA Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre Etat qui est un Etat membre de l'OAPI et un Etat contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)

Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée):

- | | |
|--|---|
| <input type="checkbox"/> AL Albanie | <input type="checkbox"/> LT Lituanie |
| <input type="checkbox"/> AM Arménie | <input type="checkbox"/> LU Luxembourg |
| <input type="checkbox"/> AT Autriche | <input type="checkbox"/> LV Lettonie |
| <input checked="" type="checkbox"/> AU Australie | <input type="checkbox"/> MD République de Moldova |
| <input type="checkbox"/> AZ Azerbaïdjan | <input type="checkbox"/> MG Madagascar |
| <input type="checkbox"/> BA Bosnie-Herzégovine | <input type="checkbox"/> MK Ex-République yougoslave de Macédoine |
| <input type="checkbox"/> BB Barbade | |
| <input type="checkbox"/> BG Bulgarie | <input type="checkbox"/> MN Mongolie |
| <input type="checkbox"/> BR Brésil | <input type="checkbox"/> MW Malawi |
| <input type="checkbox"/> BY Bélarus | <input type="checkbox"/> MX Mexique |
| <input checked="" type="checkbox"/> CA Canada | <input type="checkbox"/> NO Norvège |
| <input type="checkbox"/> CH et LI Suisse et Liechtenstein | <input type="checkbox"/> NZ Nouvelle-Zélande |
| <input checked="" type="checkbox"/> CN Chine | <input type="checkbox"/> PL Pologne |
| <input type="checkbox"/> CU Cuba | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> CZ République tchèque | <input type="checkbox"/> RO Roumanie |
| <input type="checkbox"/> DE Allemagne | <input type="checkbox"/> RU Fédération de Russie |
| <input type="checkbox"/> DK Danemark | <input type="checkbox"/> SD Soudan |
| <input type="checkbox"/> EE Estonie | <input type="checkbox"/> SE Suède |
| <input type="checkbox"/> ES Espagne | <input type="checkbox"/> SG Singapour |
| <input type="checkbox"/> FI Finlande | <input type="checkbox"/> SI Slovénie |
| <input type="checkbox"/> GB Royaume-Uni | <input type="checkbox"/> SK Slovaquie |
| <input type="checkbox"/> GE Géorgie | <input type="checkbox"/> SL Sierra Leone |
| <input type="checkbox"/> GH Ghana | <input type="checkbox"/> TJ Tadjikistan |
| <input type="checkbox"/> GM Gambie | <input type="checkbox"/> TM Turkménistan |
| <input type="checkbox"/> GW Guinée-Bissau | <input type="checkbox"/> TR Turquie |
| <input type="checkbox"/> HU Hongrie | <input type="checkbox"/> TT Trinité-et-Tobago |
| <input type="checkbox"/> ID Indonésie | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> IL Israël | <input type="checkbox"/> UG Ouganda |
| <input type="checkbox"/> IS Islande | <input checked="" type="checkbox"/> US Etats-Unis d'Amérique |
| <input checked="" type="checkbox"/> JP Japon | |
| <input type="checkbox"/> KE Kenya | <input type="checkbox"/> UZ Ouzbékistan |
| <input type="checkbox"/> KG Kirghizistan | <input type="checkbox"/> VN Viet Nam |
| <input type="checkbox"/> KP République populaire démocratique de Corée | <input type="checkbox"/> YU Yougoslavie |
| <input checked="" type="checkbox"/> KR République de Corée | <input type="checkbox"/> ZW Zimbabwe |
| <input type="checkbox"/> KZ Kazakhstan | |
| <input type="checkbox"/> LC Sainte-Lucie | |
| <input type="checkbox"/> LK Sri Lanka | |
| <input type="checkbox"/> LR Libéria | |
| <input type="checkbox"/> LS Lesotho | |

Cases réservées pour la désignation (aux fins d'un brevet national) d'Etats qui sont devenus parties au PCT après la publication de la présente feuille :

Outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, sauf la désignation de _____

Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (Pour confirmer une désignation, il faut déposer une déclaration contenant la désignation en question et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION DE LA RECEPTION DE
L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

CORLU, Bernard
Bull S.A.
PC59C18/68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

26 AOUT 1998

Date d'expédition (jour/mois/année) 10 août 1998 (10.08.98)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire PCT 3630/BC	Demande internationale no PCT/FR98/01343

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL CP8 (pour tous les Etats désignés sauf US)
UGON, Michel (pour US seulement)

Date du dépôt international : 25 juin 1998 (25.06.98)
Date(s) de priorité revendiquée(s) : 26 juin 1997 (26.06.97)

Date de réception de l'exemplaire original
par le Bureau international : 03 août 1998 (03.08.98)

Liste des offices désignés :

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE
National : CN, JP, KR, US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- ☒ les délais dans lesquels doit être abordée la phase nationale
☒ la confirmation des désignations faites par mesure de précaution
☐ les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse n° de télécopieur (41-22) 740.14.35	Fonctionnaire autorisé B. Fitzgerald n° de téléphone (41-22) 338.83.38
---	--

RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter de la date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette élection ait été effectuée avant l'expiration du 19^e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. Il appartient au déposant de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre 1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation, il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

MICROPROCESSEUR OU MICROCALCULATEUR IMPREVISIBLE

5

La présente invention concerne un microprocesseur ou microcalculateur imprévisible.

Il est connu que les microprocesseurs ou les microcalculateurs exécutent séquentiellement des instructions successives d'un programme enregistré dans une mémoire, en synchronisme avec un ou plusieurs
10 signaux de cadencement référencés par rapport à un des signaux d'horloge fournis au microprocesseur ou au microcalculateur, soit en interne, soit en externe.

Il s'est avéré possible de connaître les différentes phases de cette
15 exécution de programme en fonction du temps puisque l'exécution des instructions s'effectue séquentiellement suivant un processus prédéterminé par ce programme, en général en synchronisme avec les signaux d'horloge qui cadencent régulièrement le processeur. En effet, tout programme se traduit par une suite d'instructions qui doivent être exécutées
20 successivement dans un ordre connu à l'avance, les instants de début et de fin de chaque instruction étant parfaitement connus car elles s'exécutent suivant un processus prédéterminé en fonction du temps. Il est donc en principe possible de savoir quelle est l'instruction qui s'exécute à un moment donné dans l'unité de traitement du processeur puisque le programme qui se
25 déroule est constitué de cette suite prédéterminée d'instructions.

On peut, par exemple déterminer le nombre d'instructions exécutées à partir du lancement du programme, du démarrage de l'unité de traitement, ou encore du temps qui s'est écoulé depuis un événement, un signal de référence externe ou interne, ou encore la remise à zéro du processeur.

30 Cette possibilité de pouvoir observer le déroulement d'un programme dans un microprocesseur ou un microcalculateur est un

inconvenient majeur lorsque ce microprocesseur ou microcalculateur est utilisé dans des applications de haute sécurité. En effet, un individu mal intentionné pourrait ainsi connaître les états successifs dans lesquels se trouve le processeur et tirer parti de ces informations pour connaître certains résultats sensibles de traitement interne.

On peut imaginer, par exemple, qu'une action donnée peut se produire à des instants différents en fonction du résultat d'une opération sécuritaire déterminée, tel que le test d'une information confidentielle interne ou le déchiffrement d'un message, ou encore le contrôle d'intégrité de certaines informations. Selon l'instant considéré, on pourrait, par exemple agir sur le processeur, ou obtenir la valeur de certains registres par investigation physique afin d'obtenir des renseignements sur le résultat ou sur le contenu confidentiel de l'information, et même dans le cas de calculs cryptographiques, sur la clé secrète de chiffrement utilisée.

Il est connu des dispositifs qui apportent un premier perfectionnement aux microcalculateurs sécurisés en les dotant de circuits qui génèrent des impulsions d'horloge aléatoires. De cette manière, l'observation des événements rend particulièrement difficiles les investigations, puisque leur synchronisation devient vite impraticable.

Cependant, ce type de solution présente de nombreux inconvénients:

Tout d'abord, la conception de tels circuits est particulièrement délicate et fastidieuse car il n'est pas possible de simuler un fonctionnement aléatoire dans la totalité d'un circuit aussi complexe qu'un microcalculateur. Il est encore plus difficile de tester ces circuits en fin de fabrication dans leur comportement brouillé. Une suite aléatoire d'impulsions d'horloge est en effet très difficile à simuler pour la mise au point des circuits, mais il est encore plus difficile de maîtriser tous les comportements de l'ensemble des circuits logiques du processeur, notamment pendant les périodes de commutation des signaux sur les bus internes et dans les registres.

C'est pourquoi un premier perfectionnement, objet de la demande de brevet français N° 9602903 du 07-03-96 de la demanderesse, intitulé "circuit intégré perfectionné, procédé d'utilisation d'un tel circuit intégré", a été apporté pour permettre un fonctionnement normal du processeur pendant
5 les périodes de mise au point et de test avec une horloge périodique habituelle; le processeur étant capable de commuter lui-même le mode protégé ou le mode normal. Pour assurer la sécurité, on peut facilement imaginer que ce mode ne peut être activé par le processeur que sur
présentation d'un mot de passe ou d'un message chiffré ad-hoc.

10 En sus des difficultés citées, subsiste celle du diagnostic des pannes lors des séquences sous contrôle d'une horloge aléatoire, c'est-à-dire parfaitement désordonnée. En effet, comment peut-on, dans un tel désordre, attribuer le problème à une partie défaillante et déterminer dans
quelles conditions exactes il apparaît.

15 On voit que l'utilisation d'une horloge aléatoire, même si elle apporte un perfectionnement théoriquement intéressant, n'apporte pas une solution parfaitement satisfaisante et surtout facile à mettre en oeuvre dans la
pratique.

20 C'est un des buts de l'invention que de doter le processeur de moyens interdisant le type d'investigation décrit plus haut, et plus généralement d'empêcher les observations illicites du comportement interne du processeur tout en utilisant des circuits standards parfaitement maîtrisés, permettant une conception simple et un diagnostic des défauts reposant sur
le méthodes classiques.

25 Ce but est atteint par le fait que le microprocesseur ou microcalculateur imprévisible, comprenant un processeur, une première mémoire de travail, une mémoire principale contenant un système d'exploitation, un programme principal et un programme secondaire est caractérisé en ce qu'il possède également :

30 - une seconde mémoire de travail;

- des moyens de commutation permettant, pendant l'exécution des programmes, de commuter l'utilisation comme mémoire de travail vers l'une de ses deux mémoires de travail, tout en conservant leur contenu;

- 5 - ces moyens de commutation comprenant au moins un bloc de registres de mémorisation du contexte de déroulement des programmes dans la mémoire principale et un circuit d' aiguillage pour la validation d'une des mémoires de travail et des registres d'accès associés à chaque mémoire et contrôlés par ledit circuit d'aiguillage

10 Selon une autre particularité, il possède un second bloc de registres de mémorisation du contexte de déroulement du programme secondaire.

 Selon une autre particularité, il possède des moyens de décorrélation du déroulement des programmes par rapport à une horloge isochrone.

15 Un autre but de l'invention est de faire en sorte que la mise en oeuvre de ces moyens soit assurée par le processeur lui-même, de telle sorte que la sécurité supplémentaire créée par les moyens ci-dessus ne dépende que d'une décision du système d'exploitation situé dans le microcalculateur et par conséquent soit imprévisible pour un fraudeur.

20 Ce but est atteint par le fait que le programme principal peut autoriser ou inhiber le ou les mécanismes de commutation, par chargement du circuit de validation des mémoires de travail et des blocs de registres de mémorisation associés à chaque mémoire de travail.

25 Selon une autre particularité, la deuxième mémoire de travail et ses registres d'accès se substituent, dans son utilisation par un programme principal, à la première mémoire et ses propres registres d'accès.

 Un troisième but de l'invention est de rendre le temps d'exécution indépendant du programme lui-même sans pour autant être obligé d'utiliser des signaux d'horloge et de cadencement aléatoires.

30 Ce but est atteint par le fait que les moyens de décorrélation comprennent un générateur aléatoire permettant de déclencher par le circuit

d'interruption une interruption aléatoire de désynchronisation de l'exécution des programmes dans le processeur, par branchement aléatoire sur le programme secondaire.

5 Selon une autre particularité, les moyens de décorrélation comprennent un système de comptage de temps indépendant du processeur 1 permettant à la fin du comptage de temps de déclencher une interruption pour revenir du programme secondaire au programme principal.

10 Selon une autre particularité, le moyen de commutation des mémoires de travail est commandé soit par le processeur et son programme, soit par le système d'interruption aléatoire, soit par un compteur de temps, soit encore par une combinaison quelconque d'au moins deux parmi les trois.

15 Un quatrième but de l'invention est d'éviter que les commutations de registres ne puissent être interprétées pour accéder directement ou indirectement aux informations sensibles.

Ce but est atteint par le fait que le moyen de commutation des mémoires de travail est validé par le chargement à partir du processeur exécutant une séquence du programme principal.

20 Selon une autre particularité, le programme secondaire utilise un espace de travail identique à celui du programme principal dans la mémoire principale.

Selon une autre particularité, le programme secondaire utilise un espace de travail plus petit que celui du programme principal.

25 Selon une autre particularité, le moyen de commutation effectue la substitution des mémoires de travail et des contextes associés, à l'intérieur du cycle d'exécution d'une instruction du microprocesseur.

Selon une autre particularité, le programme secondaire ne modifie pas le contexte général de fonctionnement du programme principal afin de permettre le retour à ce dernier sans avoir à rétablir ce contexte.

30 Selon une autre particularité, le contexte du programme principal est rétabli soit automatiquement par le programme secondaire, soit

automatiquement par le moyen de commutation, avant de redonner le contrôle au programme principal.

Selon une autre particularité, il comporte des moyens de substitution de la mémoire du programme secondaire à la mémoire du programme principal.

Selon une autre caractéristique, le programme principal peut utiliser alternativement ou simultanément la première mémoire de travail et/ou la seconde mémoire de travail.

Selon une autre caractéristique, le chargement du circuit d'aiguillage permet le masquage ou le démasquage des interruptions de décorrélation.

Selon une autre caractéristique, le retour au programme principal s'effectue par une interruption déclenchée par le programme secondaire après que le registre d'aiguillage ait été convenablement chargé, par exécution d'une instruction du programme principal ou du programme secondaire, pour démasquer les interruptions.

Selon une autre particularité, il est réalisé dans un circuit intégré monolithique.

D'autres particularités et avantages de la présente invention apparaîtront plus clairement à la lecture de la description ci-après faite en référence aux dessins annexés dans lesquels :

La figure 1 représente le schéma électronique du circuit intégré selon un des modes de réalisation de l'invention;

La figure 2 représente le diagramme temporel de l'exécution d'instructions lors de l'apparition des interruptions et la prise en compte de l'interruption non masquée;

La figure 3 représente une variante de réalisation du circuit de chargement de l'un des registres de mémorisation du circuit intégré;

La figure 4 représente le logigramme de la partie de programme (P2) permettant le retour au fonctionnement normal du circuit.

La figure 1 représente l'un des modes de réalisation de l'invention. Le microprocesseur ou microcalculateur objet de l'invention appelé SUMIC (Self Unpredictable MICrocomputer) est constitué d'un circuit intégré monolithique comportant une unité de traitement (1), d'une mémoire (6) non volatile contenant les programmes à exécuter, une mémoire RAM (51) avec ses registres d'adresse (A2) et de données (D2) ainsi que d'un générateur de signaux aléatoires ou pseudo-aléatoires (2) qui délivre, par exemple, des impulsions à intervalles irréguliers et imprévisibles, un circuit d'interruption (4), un registre (R2), un timer (R3), un circuit séquenceur (8), une mémoire non volatile (7) (NVM), une mémoire « trompe l'oeil » (dummy memory-DUMRAM) (52) du type volatile avec ses registres d'adressage (A3) et de donnée (D3), deux piles de registres (54, 55) pour mémoriser les paramètres de retour au fonctionnement normal ainsi qu'un circuit d'aiguillage (53) constitué par exemple par un registre ayant le nombre de cellules suffisant pour contrôler le fonctionnement des registres d'adresses (A1) et (A3) et de données (D1) et (D3) et un premier bloc (54) et un deuxième bloc (55) de registres de mémorisation. Ce registre d'aiguillage (53) est chargé par l'unité de traitement (1) à travers le bus (3). L'état de ce registre d'aiguillage (53) permet notamment de valider la RAM et/ou la DUMRAM dans l'espace mémoire de travail du processeur ou hors de cet espace.

Dans ce circuit intégré monolithique, l'unité de traitement est reliée par un bus (3) aux différentes mémoires vers chaque fois un registre d'adresses respectif (A1, A2, A3) et un registre de données respectif (D1, D2, D3), chacun de ces registres d'adresses et de données étant verrouillable par une ligne de commandes (531 A, 532 A, 536 A), respectivement (531 D, 532 D, 536 D), sortant du circuit d'aiguillage (53). Ce circuit d'aiguillage comporte également trois autres lignes de commande, l'une (533) aboutissant à une porte ET (11) à deux entrées, dont la deuxième entrée reçoit une ligne du bus (31) provenant du circuit d'interruption. La sortie de cette porte ET est connectée directement à l'un des bits du registre de validation d'interruption IER (Interrupt enable

register) pour permettre le masquage de l'interruption déclenchée par le circuit d'interruption (4) uniquement lorsque le circuit d'aiguillage n'a pas été activé et lorsque par conséquent la ligne (533) n'est pas active.

Les deux autres lignes (534, 535) verrouillent chacune l'un des deux
5 blocs ou piles de registres de mémorisation (54, 55). Chacun des blocs comporte une pluralité de registres de mémorisation (54), respectivement (55), permettant le stockage des informations qui seront décrites ci-après. Ces registres (54, 55) sont reliés au bus (3) commun aux mémoires. Ce même bus (3) permet le chargement du circuit d'aiguillage (53) avec les
10 valeurs nécessaires pour rendre les lignes (531 A, 532 A, 532 D, 536 A, 536 D, 533, 534, 535) de commande actives ou inactives selon le mode de fonctionnement souhaité. La mémoire non volatile (6) contient le système d'exploitation du circuit (operating system) et un premier programme (P1) d'application, dit programme principal par la suite, ainsi qu'un second
15 programme (P2), dénommé programme secondaire par la suite, le séquenceur (8), les registres (R2), le timer (R3) et le générateur aléatoire (R1) sont également reliés au bus (3) et les trois éléments (R1, R2, R3) sont reliés à un circuit de génération d'interruption (4), lequel est branché sur les entrées d'interruption du processeur (1) en utilisant sur le registre de
20 masquage d'interruption (IER) du processeur un des bits qui, en général, se trouve réservé et disponible pour des applications spécifiques à certains utilisateurs.

Dans un premier mode de réalisation, le programme principal (P1) contenu en mémoire non volatile (6) modifie, lorsque nécessaire, l'état du
25 circuit d'aiguillage (53) par l'intermédiaire du bus (3), ce qui ne présente aucune difficulté de réalisation. Ceci met momentanément hors circuit la mémoire RAM principale de travail (51) ou une partie de cette mémoire en agissant sur l'entrée CE (chip enable) de validation d'un boîtier de mémoire, ainsi que tous les registres nécessaires du premier bloc (54), pour le retour
30 au fonctionnement normal. Ces mémoires et registres pourront être avantageusement du type statique afin d'économiser l'énergie nécessaire à

leur maintien. Le circuit d'aiguillage (53) substitue donc la mémoire « trompe-l'oeil » (52) à la mémoire principale de travail (51) afin que les programmes s'exécutant utilisent exclusivement la mémoire « trompe-l'oeil » à la place de la mémoire principale de travail. Cette mémoire « trompe-l'oeil » (52) peut être située aux mêmes adresses que la mémoire à laquelle elle se substitue, mais peut être située également à une adresse différente. Une solution avantageuse et économique consiste à utiliser une mémoire RAM de très petite taille pour cette mémoire « trompe-l'oeil ». En effet, cette mémoire « trompe-l'oeil » ne jouant aucun rôle fonctionnel pour le programme principal, on peut restreindre l'espace adressable en diminuant tout simplement la longueur du registre d'adressage (A3). On peut aussi « replier » l'adresse sur elle-même en faisant un OU-Exclusif entre plusieurs blocs du registre d'adresse. Ainsi, si l'espace adressable de la mémoire principale de travail est de 512 octets, on peut restreindre la mémoire « trompe-l'oeil » à 32 octets sans aucun problème, ce qui conduit ainsi à une réalisation très économique. Ces 32 octets peuvent correspondre, par exemple, à simplement ajouter une ligne de mémoire RAM dans la matrice de la mémoire principale de travail. Cette ligne aura dans ce cas ses propres registres d'adresse (A3) et de données (D3). Quand le circuit d'aiguillage (53) active la mémoire « trompe-l'oeil » cela peut aussi interdire tout accès en écriture dans la NVM, de façon à ne pas perturber son contenu.

On peut avantageusement, au sens de l'exécution de la commutation, utiliser alternativement deux blocs de registres, un premier bloc (54) et un second bloc (55) contenant chacun tout le contexte nécessaire à l'exécution du programme, et notamment les compteurs de programme respectivement (PC1) pour le premier bloc (54) et (PC2) pour le second bloc (55), les registres de décodage d'instruction (D1) pour le premier et (D2) pour le second ainsi que d'autres registres symbolisés par (T11, T12 et T21, T22). Ces derniers registres (T11, T12, T21 et T22) conservent les paramètres de fonctionnement, tel que par exemple le numéro du cycle machine dans lequel on doit se trouver. Tous ces registres

sont commutés automatiquement par le circuit (53) d'aiguillage. Le changement d'adresse s'effectue dans ce cas instantanément, sans être obligé, comme c'est le cas dans la plupart des microcalculateurs, de sauvegarder, par une instruction spécifique, le contenu du compteur de programme dans une pile de registres. Ainsi la commutation dans les deux sens est très rapide (en général très inférieure à un cycle d'horloge), ce qui augmente considérablement le niveau de sécurité du dispositif. Le même mécanisme peut être utilisé pour les autres registres qui sauvegardent le contexte de fonctionnement du processeur, comme (T11 à T22).

Il faut bien comprendre que lorsque le programme (P1), active par le chargement du registre d'aiguillage le fonctionnement en mode « trompe-l'oeil » du circuit intégré, ce circuit d'aiguillage (53) va bloquer la première pile de registres (54), laquelle conservera les paramètres antérieurs à l'opération « trompe-l'oeil » de fonctionnement du circuit, pour redémarrer là où le programme (P1) avait été interrompu. De son côté, la seconde pile de registres (55) sera utilisée pour permettre le fonctionnement normal du circuit avec la mémoire « trompe-l'oeil » en exécution du programme (P2). Il est bien évident également que dans ce cas le bit du registre IER de masquage des interruptions, correspondant au fonctionnement en mode « trompe-l'oeil », aura été démasqué, ceci de façon à permettre, lors de la génération d'une interruption, soit par le générateur aléatoire, soit par le timer (R3) préalablement chargé par le générateur aléatoire avec un nombre aléatoire et à la fin de l'écoulement du temps représenté par ce nombre, soit par le registre (R2) qui aura été chargé par des informations particulières, de déclencher l'interruption (31) de passage du fonctionnement normal sous le contrôle du programme (P1) au fonctionnement en mode « trompe-l'oeil » sous le contrôle du programme (P2).

La figure 2 illustre le fonctionnement en mode interruption. Le diagramme montre qu'une première impulsion d'interruption IT, émise par le circuit d'interruption sur la ligne (31) vers l'unité de traitement (1), n'est pas prise en compte car elle a été masquée en agissant sur le registre et le

masquage d'interruption par une instruction "MOVE immédiat data to register IER" de chargement de donnée dans le registre de masquage. On suppose que l'instruction en cours démasque l'interruption de déroutement (mais cela peut être fait par toute autre instruction à un instant différent). La

5 deuxième impulsion est cette fois prise en compte par l'unité de traitement (1), ce qui fait commuter le circuit d'aiguillage (53) et par voie de conséquence, le second bloc de registres (55) et la DUMRAM (52) deviennent actifs à la place du premier bloc (54) et de la mémoire « trompe-

l'oeil » RAM (51). On notera que la prise en compte de l'interruption ne peut

10 se faire que lors de la transition d'un état à un autre, par exemple entre (S2) et (S3), ceci afin de mémoriser un état stable et cohérent de la machine, et surtout de restituer exactement le même état lors du retour au programme interrompu. Si cette interruption est prise en compte, comme c'est le cas habituel, à la fin d'une instruction, il n'y a pas de problème particulier lors de

15 la reprise du programme interrompu, puisque celle-ci s'opère normalement à l'instruction suivante. Par contre, si cette interruption a lieu en cours d'exécution d'une instruction, par exemple à l'état (S2), il faut, bien entendu, que les circuits de séquençement soient rétablis à l'identique, de façon à enclencher correctement l'état (S3) lors de la reprise du programme

20 interrompu. Ceci peut par exemple être réalisé par une liaison directe entre le registre (T11) et le séquenceur (8) par l'intermédiaire du bus (3) au moment de la reprise. Cette liaison peut également être spécifique sans passer par le bus (S3). On peut aussi avantageusement mettre les registres de mémorisation d'état dans le séquenceur lui-même, ce qui évite la

25 mobilisation du bus pendant cette phase.

De cette manière, par une interruption, le programme principal (P1) peut autoriser et/ou provoquer la commutation sur un programme secondaire (P2) ainsi que décrit plus bas. Quand le programme secondaire n'est plus

30 actif, l'état du circuit d'aiguillage (53) est changé et la mémoire de travail RAM retrouve sa configuration première sans modification, ce qui permet au

programme principal de reprendre son cours exactement au point où il avait été interrompu. On peut aussi faire en sorte que lorsque le programme principal (P1) veut se protéger, il déclenche par déroutement lui-même un programme secondaire (P2) qui engendre un traitement de longueur aléatoire à des instants choisis par lui, soit au début soit en cours de traitement de façon à brouiller les différentes séquences. Le fonctionnement du processeur peut alors être piloté par le programme secondaire (P2) qui peut, par exemple, déclencher une boucle d'attente dont le temps dépend d'un nombre aléatoire issu du générateur (2). Le programme secondaire peut s'exécuter en utilisant les parties de mémoire non utilisées par le programme principal afin que ce dernier puisse reprendre son cours normal soit dès que le programme secondaire lui transmet à nouveau le contrôle soit encore à la prochaine interruption, soit encore en utilisant le timer comme précédemment, ou soit en utilisant une combinaison des deux. Le programme secondaire peut aussi utiliser des ressources communes à condition qu'il rétablisse le contexte du programme principal avant de lui redonner le contrôle.

On pourrait être tenté de dire que ces mécanismes s'apparentent à l'exécution d'un branchement de programme principal vers un programme secondaire avec retour en fin d'exécution de ce dernier mais celui de l'invention est très différent:

- le programme secondaire n'exécute aucune fonction obligatoirement en relation avec le programme principal.
- la taille de la mémoire « trompe-l'oeil » (52) peut être beaucoup plus petite que celle nécessaire au déroulement normal d'un programme.
- le contenu de la mémoire « trompe-l'oeil » (52) n'a aucune importance car elle ne sert qu'à brouiller les pistes.
- il est possible, avec ce mécanisme rapide, d'entrelacer les instructions de programme secondaire avec celles du programme principal.
- il n'est pas nécessaire de sauver le contexte du programme secondaire, puisque ce dernier ne sert qu'à brouiller les pistes.

Dans un deuxième mode de réalisation, lorsque le processeur fait commuter le circuit (53), il active en même temps un timer (R3) initialisé soit à l'aide du générateur aléatoire (2), soit à partir du contenu de la mémoire non volatile NVM (7). Cette NVM du type E2 PROM, par exemple ou ferro-
 5 électrique, peut en effet contenir un nombre unique modifié à chaque utilisation de la NVM. Quand le timer (R3) arrive à échéance au bout d'un temps imprévisible, il déclenche le retour au programme principal en commutant aussi le circuit d'aiguillage (53) pour remettre la mémoire principale dans l'espace de travail. Ce mécanisme peut s'exécuter, soit par
 10 le biais d'une interruption classique, soit encore par une action directe du timer (R3) sur le circuit d'aiguillage (53) et par action sur les registres (PC1) et (PC2) contrôlant l'exécution des programmes par l'unité de traitement (1) tels que (PC1) et (PC2).

Dans une variante, il est possible d'utiliser pour le programme
 15 secondaire (P2), une partie quelconque du programme principal (P1) en pointant au départ sur une adresse au hasard et en réalisant une inversion des octets qui sont issus de l'adresse et/ou en inversant, par exemple, le contenu du registre (ID2) par câblage à l'envers ou encore par un circuit de décalage à gauche du contenu d'une adresse. On aura ainsi l'assurance
 20 que ce programme exécutera des instructions complètement fantaisistes.

Une autre variante pour permettre l'exécution d'instructions fantaisistes pourra être constituée par la figure 3 dans laquelle un registre de décodage d'instructions temporaire IDT est relié, d'une part au bus (3) par une portion de bus (33) et d'autre-part, à la seconde pile de registres
 25 (55) permettant la mémorisation des états du circuit par une portion de bus (34). La portion de bus (34) est reliée matériellement au registre (ID2) de la pile (55) par un câblage particulier qui relie le bit (B7) du registre IDT au bit (B4) du registre (ID2), le bit (B6) du registre IDT au bit (B1) du registre (ID2), le bit (B5) du registre IDT au bit (B3) du registre (ID2), etc.

30 Enfin, une dernière variante permettant l'exécution (d'instructions) complètement fantaisistes est constituée par le mode de réalisation de la

figure 3B dans lequel le bus (3) est relié par une portion de bus (35) au registre IDT de décodage d'instructions temporaires. Une autre portion (37) de bus relie ce registre IDT à une porte OU-Exclusif (39) à plusieurs entrées. Les autres entrées de cette porte OU étant reliées par un bus (38) à

5 un registre (R'2) chargé par une portion (36) de bus qui le met en relation avec le bus (3). Ce registre (R'2) peut être chargé avec toute information telle que celle provenant du générateur aléatoire (R1), ou du timer, ou de la mémoire non volatile NVM (7) par une instruction "MOVE register (R1) (par exemple) to register (R'2)". Ce type d'instructions de déplacement est bien

10 connu de l'homme de métier du domaine des microprocesseurs et ne pose aucune difficulté de mise en oeuvre. Le OU-Exclusif entre les informations provenant du registre (R'2) et les valeurs chargées dans le registre IDT permet de modifier totalement les instructions du programme (P2) et ainsi d'exécuter des instructions complètement fantaisistes.

15 On peut aussi utiliser dans le programme (P2) une pluralité de séquences qui seront appelées de façon aléatoire et chacune de ces séquences mettra en oeuvre un ensemble d'instructions différentes qui entraîneront un temps de traitement variable dans chaque branche et des comportements différents du microprocesseur. Les séquences pourront être

20 appelées de façon aléatoire, par exemple, après que le programme principal ait effectué le saut au programme secondaire, ce dernier charge une valeur aléatoire V provenant de la mémoire (7) dans deux registres, par exemple, (T21) et (T22) du microprocesseur (1). Le programme secondaire incrémente cette valeur V, puis le programme commande la mémorisation de

25 cette valeur incrémentée dans la mémoire non volatile (7). Cette valeur mémorisée dans la mémoire non volatile (7) est destinée à une utilisation ultérieure. Le programme secondaire prélève ensuite n bits de poids forts ou faibles dans (T21) afin d'obtenir une valeur r qui permettra de désigner la séquence de programme à exécuter parmi les différentes séquences de

30 programme secondaire.

Dans un troisième mode de réalisation, le générateur aléatoire (2) est interrogeable par le processeur (1) à travers le bus (3) par une instruction de lecture afin de connaître son état, soit en lisant directement une impulsion déterminée, soit en regroupant plusieurs, soit encore en considérant le contenu du registre (R2) chargé à partir du générateur aléatoire (2). Lorsque le programme principal veut se protéger, il passe le contrôle au programme secondaire d'une façon similaire au mécanisme vu précédemment.

Bien entendu, il est possible de combiner les effets des modes de réalisation précédents, en ayant, d'une part une horloge aléatoire et d'autre part, la possibilité d'interrompre le déroulement du programme principal, soit par lui-même, soit par un système d'interruption aléatoire qu'il autorise ou non.

On voit ainsi que le déroulement du programme principal est réalisé selon un séquençement absolument imprévisible qui dépend, soit du générateur aléatoire, soit du programme, soit du timer, soit du programme secondaire, soit encore de deux, trois ou quatre éléments à la fois. Lorsque le programme principal exécute des fonctions non sensibles sur le plan sécuritaire, il peut ainsi recourir au fonctionnement normal, par exemple pour délivrer des résultats au monde extérieur ou encore masquer les interruptions de décorrélation du timer (R3) ou du générateur aléatoire (2) de façon à optimiser le temps de traitement. Dès qu'une fonction sécuritaire est mise en oeuvre, le programme principal (P1) autorise le fonctionnement en mode aléatoire en validant les interruptions de décorrélation afin de "brouiller" le fonctionnement.

Un quatrième mode de réalisation, illustré également par la figure 1 permet d'utiliser les mémoires RAM (51) et (52) en simultanéité. En effet, si l'on suppose que l'on puisse arriver à détecter les commutations des mémoires et des registres associés, on pourrait éventuellement faire une analyse en éliminant les séquences utilisant la mémoire « trompe-l'oeil » (52). Pour éviter cet éventualité, ce mode de réalisation permet de valider

simultanément les mémoires (51) et (52) en parallèle pendant une première phase. Ceci suppose, bien entendu, que la mémoire (52) possède, dans ce cas, une taille au moins égale à celle de la zone utilisée par le programme (P1) dans la mémoire (51) lorsqu'il travaille avec cette dernière. De cette

5 manière, les contenus des deux zones de mémoire utilisées par le programme (P1) respectivement dans les mémoires (51) et (52) sont initialisés et utilisés par ce programme de façon identique pendant cette première phase. Une variante peut consister à ne valider par chargement du circuit d'aiguillage (53) avec la configuration nécessaire que l'un des deux

10 registres (D2) ou (D3) pendant les cycles de lecture, pour éviter les éventuels conflits, mais cela ne change pas fondamentalement l'invention. On ne peut donc distinguer quelle est la mémoire qui sert réellement pendant cette phase. Il est alors possible, pendant une deuxième phase, de commuter les mémoires alternativement et de façon aléatoire par des

15 modifications du registre du circuit d'aiguillage (53), tout en continuant d'exécuter le même programme (P1). On ne pourra donc plus corréler l'exécution d'un programme ou d'un autre avec la RAM ou les registres utilisés. Dans une troisième phase, on commute sur la mémoire « trompe-l'oeil » (52) en passant sur le programme (P2) comme décrit précédemment,

20 et ce, à des instants imprévisibles, le retour à la mémoire principale de travail (51) s'effectue aussi à des instants imprévisibles, le processus pouvant se reproduire à volonté sous le contrôle du programme principal (T1) qui veut se protéger.

Enfin, le dernier problème posé par l'invention consiste à pouvoir

25 quitter le mode « trompe-l'oeil » du programme (P2) pour revenir au mode de fonctionnement normal avec le programme (P1). Juste avant de passer le contrôle au programme (P2), le programme (P1) autorise les interruptions provenant soit du générateur aléatoire, soit du timer, non sans savoir initialisé ce dernier. Pendant le déroulement du programme anarchique (P2),

30 survient alors une interruption par le circuit (4) qui passe la main à un programme d'interruption (PIT). Ce programme, qui est accédé de façon

classique par l'intermédiaire d'un vecteur d'interruption, analyse par exemple le contexte d'exécution du programme en cours. Si (P2) est actif, PIT repasse le contrôle au programme (P1). Ce mécanisme peut s'effectuer de la façon suivante : lors de l'exécution des premières instructions du

5 programme PIT, celui-ci peut par exemple être constitué, comme représenté à la figure 4, par une lecture (41) du contenu du circuit d'aiguillage (53) puis un test (42) pour déterminer si les informations contenues dans le circuit (53) correspondent au fonctionnement en mode « trompe-l'oeil ». Dans l'affirmative, le programme PIT exécute une instruction de retour au

10 programme (P1) représenté par l'étape (43), ce retour est provoqué par l'écriture du registre d'aiguillage (53) selon l'étape (44) qui consiste à modifier les valeurs des lignes (534) et (531). Cette nouvelle écriture (44) dans le registre d'aiguillage (53) permet de revenir en mode normal modifié les valeurs de la ligne (534) et de la ligne (531) de façon à autoriser à

15 nouveau l'utilisation de la pile (54) et de la mémoire de travail principale (51). Cette instruction de retour au programme (P1) peut s'exécuter directement après le test « trompe-l'oeil » (42) ou après l'exécution d'un certain nombre d'autres instructions non représentées qui permettent de générer un temps aléatoire. Dans le cas où le test (42) est négatif, le

20 programme se poursuit à l'étape (45) par une écriture du registre d'aiguillage (53) pour basculer en mode « trompe-l'oeil » de façon à modifier les valeurs des lignes (535) et (532) pour autoriser l'utilisation de la pile de registre (55) et de la mémoire « trompe-l'oeil » et de façon à verrouiller les circuits commandés par les (531) et (534).

25 On remarquera, que dans tous ces modes de réalisation, il n'est pas nécessaire d'utiliser une horloge aléatoire. Au contraire, la distribution d'horloge peut rester tout à fait classique et isochrone, ce qui permet une conception facile des circuits ainsi que leur simulation et leur test. En fait, la sécurité ne provient plus du fait que le processeur est cadencé

30 aléatoirement, elle se situe au niveau de l'exécution proprement dite des

programmes, et ceci en synchronisme ou non avec une horloge isochrone; c'est l'exécution elle même qui est brouillée.

L'organisation des programmes exécutés par le processeur peut être réalisée de telle manière que le fonctionnement du processeur soit piloté par
5 un véritable système d'exploitation sécuritaire qui décide du type de brouillage à mettre en oeuvre en fonction du type de programme exécuté par la machine. Dans ce cas c'est le système d'exploitation qui gère comme bon lui semble les divers signaux provenant du générateur aléatoire, des interruptions, du lancement des programmes principal et secondaire. Il est
10 clair que le programme secondaire peut être utilisé pour réaliser d'autres fonctions qu'une simple boucle d'attente, notamment des traitements qui peuvent être utiles au programme principal, de façon à tirer parti du temps dédié au programme secondaire, ces traitements pouvant être constitués , par exemple, par des préparations de calculs utilisés ultérieurement par le
15 programme principal. Bien entendu, on peut facilement généraliser les mécanismes de l'invention lorsque le processeur fonctionne en multi-application, les programmes d'application pouvant alors être considérés comme autant de programmes principaux.

Le générateur aléatoire et le timer vus plus haut ne posent pas de
20 problèmes particuliers de réalisation et sont connus de l'homme de l'art lorsqu'ils sont utilisés séparément pour d'autres usages n'ayant aucun lien avec l'invention.

Pour le générateur aléatoire, on peut, par exemple, utiliser des compteurs rebouclés ayant des périodes différentes. ces compteurs étant
25 initialisés par une information d'initialisation stockée en mémoire non volatile (7). Lorsque le processeur démarre, les compteurs prennent en compte la valeur stockée comme valeur de départ. En cours de calcul ou à la fin, la mémoire non volatile est mise à jour avec une nouvelle valeur qui va servir d'information d'initialisation pour initialiser les compteurs à la prochaine
30 initialisation. La génération des impulsions d'interruption vues plus haut peut alors se produire lorsque le nombre généré possède certaines

- caractéristiques telles que l'égalité avec certaines données du programme. On peut aussi prendre la valeur d'un ou plusieurs bits d'un ou plusieurs compteurs. Il est également possible de réaliser un très bon générateur aléatoire en utilisant un algorithme cryptographique ou une fonction de hachage, initialisés par l'information d'initialisation vue plus haut. Dans ce cas, le générateur peut être réalisé sous la forme d'un programme mettant en oeuvre l'algorithme. On voit facilement que ce générateur de nombre aléatoire peut être également utilisé pour engendrer les divers nombres aléatoires vus plus haut. Une autre manière de réaliser un tel générateur est d'amplifier la tension engendrée aux bornes d'une diode dite "de bruit " et de mettre en forme les signaux après un filtrage passe bas pour éviter que les impulsions de bruit trop rapide ne perturbent le fonctionnement du microprocesseur.

REVENDICATIONS

1. Microprocesseur ou microcalculateur imprévisible, comprenant un
5 processeur (1), une première (51) mémoire de travail, une mémoire principale (6) contenant un système d'exploitation, un programme principal (P1) et un programme secondaire (P2), caractérisé en ce qu'il possède également :

- une seconde (52) mémoire de travail;
- 10 - des moyens de commutation permettant, pendant l'exécution des programmes, de commuter l'utilisation comme mémoire de travail vers l'une de ses deux mémoires de travail (51, 52), tout en conservant leur contenu;
- ces moyens de commutation comprenant au moins un bloc de registres (54) de mémorisation du contexte de déroulement des programmes
15 dans la mémoire principale et un circuit d'aiguillage (53) pour la validation d'une des mémoires de travail et des registres d'accès (A1-A3), (D1-D3) associés à chaque mémoire (51, 52, 6) et contrôlés par ledit circuit d'aiguillage (53).

2. Microprocesseur ou microcalculateur imprévisible selon la
20 revendication 1, caractérisé en ce qu'il possède un second bloc de registres (55) de mémorisation du contexte de déroulement du programme secondaire.

3. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce qu'il possède des moyens
25 (R1, R2, R3) de décorrélation du déroulement des programmes par rapport à une horloge isochrone.

4. Microprocesseur ou microcalculateur selon l'une des revendications précédentes, caractérisé en ce que le programme principal peut autoriser ou inhiber le ou les mécanismes de commutation, par
30 chargement du circuit (53) d'aiguillage et de validation des mémoires de

travail (51, 52) et des blocs de registres de mémorisation (54,55) associés à chaque mémoire de travail (51, 52) respective.

5 5. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce que la deuxième mémoire de travail (52) et ses registres d'accès (A3, D3) se substituent dans son utilisation par un programme principal, à la première mémoire (51) et ses propres registres d'accès (A2, D2).

10 6. Microprocesseur ou microcalculateur imprévisible selon la revendication 3, caractérisé en ce que les moyens de décorrélation comprennent un générateur aléatoire (2) permettant de déclencher par le circuit d'interruption (4) une interruption aléatoire de désynchronisation de l'exécution des programmes dans le processeur, par branchement aléatoire sur le programme secondaire (P2).

15 7. Microprocesseur ou microcalculateur selon les revendications 4 ou 6, caractérisé en ce que les moyens de décorrélation comprennent un système de comptage de temps (R3) indépendant du processeur (1) permettant à la fin du comptage de temps de déclencher une interruption pour revenir du programme secondaire au programme principal.

20 8. Microprocesseur ou microcalculateur imprévisible selon les revendications 4, ou 6, ou 7 ou leur combinaison, caractérisé en ce que le moyen de commutation (53, 54, 55, A2, A3, D2, D3)) des mémoires de travail est commandé, soit par le processeur et son programme, soit par le système d'interruption aléatoire (2, 4), soit par un compteur de temps (R3), soit encore par une combinaison quelconque d'au moins deux parmi les
25 trois.

9. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes ou de leur combinaison, caractérisé en ce que le moyen de commutation (53, 54, 55, A2, A3, D2, D3), des mémoires de travail est validé par le chargement à partir du processeur (1) exécutant une
30 séquence du programme principal.

10. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce que le programme secondaire (P2) utilise un espace de travail identique à celui du programme principal (P1) dans la mémoire principale (6).

5 11. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications 1 à 9, caractérisé en ce que le programme secondaire (P2) utilise un espace de travail plus petit que celui du programme principal (P1).

10 12. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce que le moyen de commutation effectue la substitution des mémoires de travail (51, 52, 53, 54, 55, A2, A3, D2, D3)) et des contextes associés, à l'intérieur du cycle d'exécution d'une instruction du microprocesseur.

15 13. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce que le programme secondaire (P2) ne modifie pas le contexte général de fonctionnement du programme principal (P1) afin de permettre le retour à ce dernier sans avoir à rétablir ce contexte.

20 14. Microprocesseur ou microcalculateur imprévisible selon la revendication 13, caractérisé en ce que le contexte du programme principal (P1) est rétabli soit automatiquement par le programme secondaire (P2), soit automatiquement par le moyen de commutation (53), avant de redonner le contrôle au programme principal (P1).

25 15. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce qu'il comporte des moyens de substitution de la mémoire du programme secondaire (P2) à la mémoire du programme principal (P1).

30 16. Microprocesseur ou microcalculateur imprévisible selon l'une des revendications précédentes, caractérisé en ce que le programme principal (P1) peut utiliser alternativement ou simultanément la première mémoire de travail (51) et/ou la seconde mémoire de travail (52).

17. Microprocesseur ou microcalculateur imprévisible, caractérisé en ce que le chargement du circuit d'aiguillage (53) permet le masquage ou le démasquage des interruptions de décorrélation.

5 18. Microprocesseur ou microcalculateur imprévisible, caractérisé en ce que le retour au programme principal (P1) s'effectue par une interruption déclenchée par le programme secondaire (P2) après que le registre d'aiguillage (53) ait été convenablement chargé, par exécution d'une instruction du programme principal (P1) ou du programme secondaire (P2), pour démasquer les interruptions.

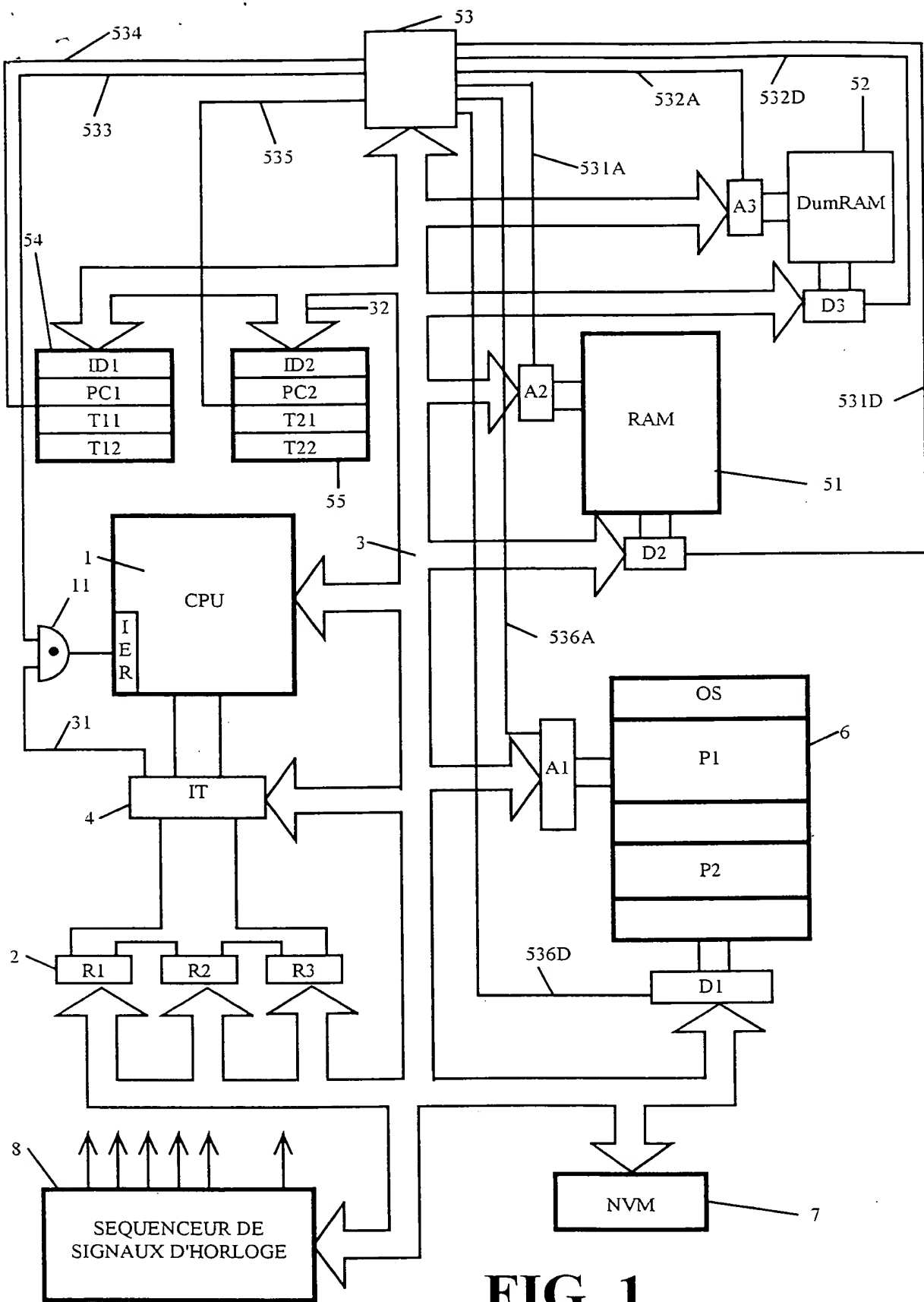
10 19. Microprocesseur ou microcalculateur imprévisible, caractérisé en ce qu'il est réalisé dans un circuit intégré monolithique.

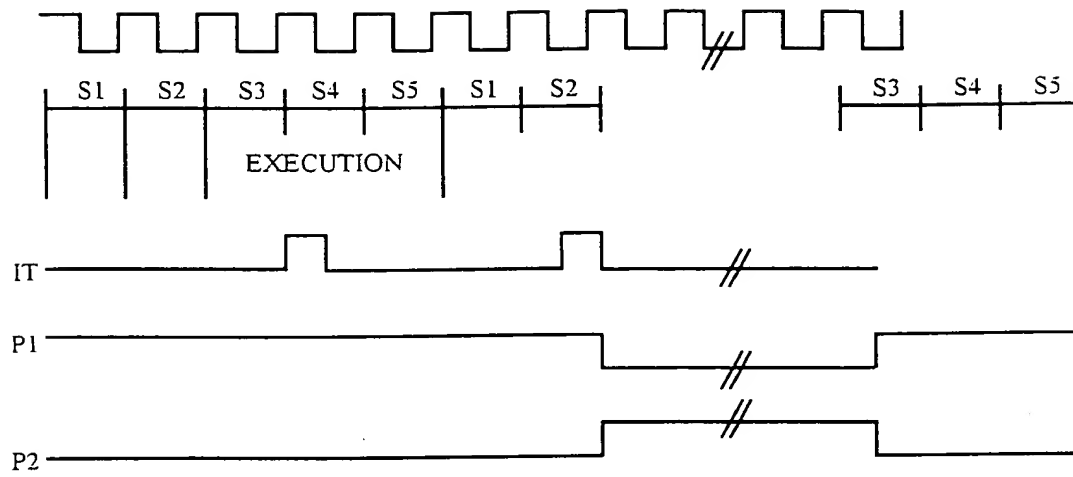
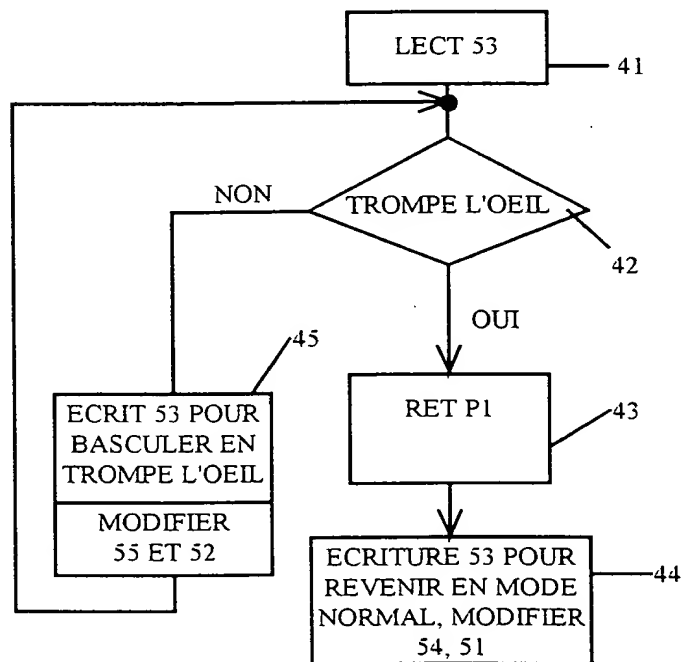
ABREGE

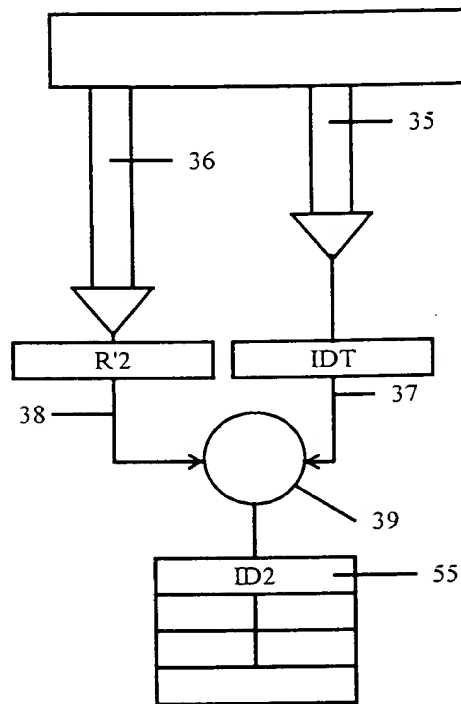
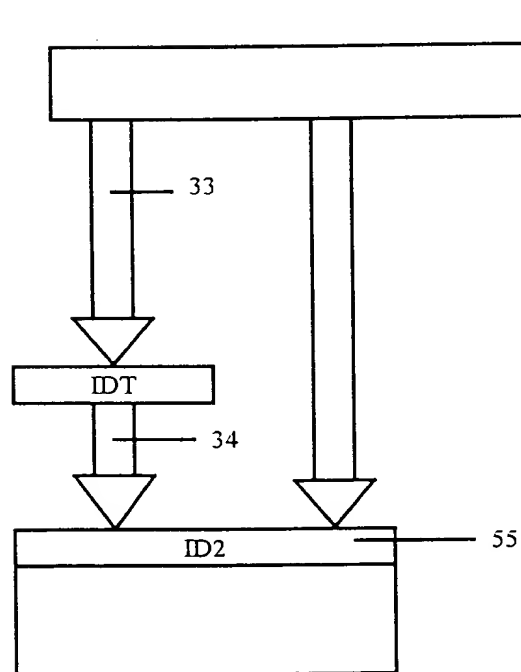
La présente invention concerne un microprocesseur ou microcalculateur imprévisible, comprenant un processeur (1), une première
5 (51) mémoire de travail, une mémoire principale (6) contenant un système d'exploitation, un programme principal (P1) et un programme secondaire (P2), caractérisé en ce qu'il possède également :

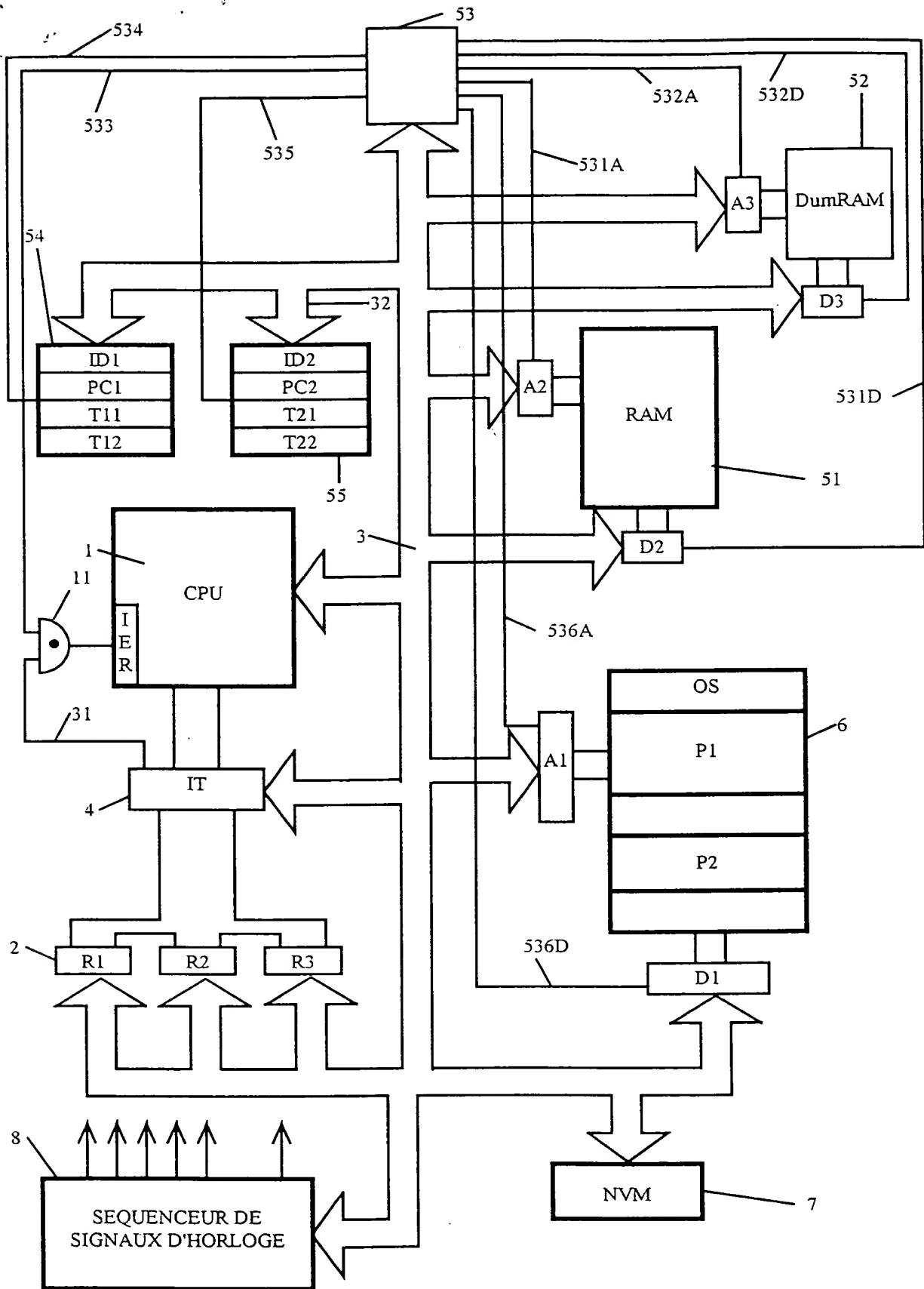
- une seconde (52) mémoire de travail;
- des moyens de commutation permettant, pendant l'exécution des
10 programmes, de commuter l'utilisation comme mémoire de travail vers l'une de ses deux mémoires de travail (51, 52), tout en conservant leur contenu;
- ces moyens de commutation comprenant au moins un bloc de registres (54) de mémorisation du contexte de déroulement des programmés dans la mémoire principale et un circuit d' aiguiillage (53) pour la validation
15 d'une des mémoires de travail et des registres d'accès (A1-A3), (D1-D3) associés à chaque mémoire (51, 52, 6) et controlés par ledit circuit d'aiguiillage (53).

Figure 1

**FIG. 1**

**FIG. 2****FIG. 4**

**FIG. 3B****FIG. 3A**



PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire PCT 3630/BC	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER	
Demande internationale n° PCT/FR 98/ 01343	Date du dépôt international (jour/mois/année) 25/06/1998	(Date de priorité (la plus ancienne) (jour/mois/année) 26/06/1997
Déposant BULL CP8 et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).
2. ☐ Il y a absence d'unité de l'invention (voir le cadre II).
3. ☐ La demande internationale contient la divulgation d'un listage de séquence de nucléotides ou d'acides aminés et la recherche internationale a été effectuée sur la base du listage de séquence
 - ☐ déposé avec la demande internationale
 - ☐ fourni par le déposant séparément de la demande internationale
 - ☐ sans être accompagnée d'une déclaration selon laquelle il n'inclut pas d'éléments allant au-delà de la divulgation faite dans la demande internationale telle qu'elle a été déposée.
 - ☐ transcrit par l'administration
4. En ce qui concerne le titre, ☒ le texte est approuvé tel qu'il a été remis par le déposant.
☐ Le texte a été établi par l'administration et a la teneur suivante:
5. En ce qui concerne l'abrégé,
 - ☒ le texte est approuvé tel qu'il a été remis par le déposant
 - ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.
6. La figure des dessins à publier avec l'abrégé est la suivante:
 Figure n° 1 ☒ suggérée par le déposant. ☐ Aucune des figures n'est à publier.
☐ parce que le déposant n'a pas suggéré de figure.
☐ parce que cette figure caractérise mieux l'invention.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 98/01343

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G06F1/00 G06F9/46

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 135 753 A (IBM) 3 avril 1985 voir abrégé; figures voir page 5, ligne 7 - ligne 28 voir page 9, ligne 13 - page 13, ligne 6 voir revendications ----	1-6
Y	EP 0 129 693 A (IBM) 2 janvier 1985 voir abrégé; figure 1 voir page 1, ligne 1 - ligne 8 voir page 2, ligne 26 - page 4, ligne 6 voir page 9, ligne 19 - ligne 30 voir page 11, ligne 3 - ligne 15 ----- -/--	1-6

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

17 septembre 1998

Date d'expédition du présent rapport de recherche internationale

24/09/1998

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Wiltink, J

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 septembre 1991 voir abrégé voir colonne 1, ligne 29 - colonne 3, ligne 4 voir revendications 1-3 ---	3,6
A	EP 0 463 855 A (NIPPON ELECTRIC CO) 2 janvier 1992 voir abrégé; revendications; figures ---	1
A	EP 0 417 817 A (DIGITAL EQUIPMENT CORP) 20 mars 1991 voir abrégé; revendications 1-4; figure 1 -----	3,6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 98/01343

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0135753	A	03-04-1985	US 4591982 A	27-05-1986
			DE 3485205 A	28-11-1991
			JP 1464934 C	10-11-1988
			JP 60055467 A	30-03-1985
			JP 63013223 B	24-03-1988
EP 0129693	A	02-01-1985	US 4575817 A	11-03-1986
			CA 1204877 A	20-05-1986
			JP 1600728 C	31-01-1991
			JP 2026250 B	08-06-1990
			JP 60008956 A	17-01-1985
EP 0448262	A	25-09-1991	AT 152530 T	15-05-1997
			AU 637677 B	03-06-1993
			AU 7291591 A	26-09-1991
			CA 2037857 A	21-09-1991
			DE 69125881 D	05-06-1997
			DE 69125881 T	14-08-1997
			DK 448262 T	27-10-1997
			ES 2100207 T	16-06-1997
			GR 3023851 T	30-09-1997
			IE 74155 B	02-07-1997
			JP 4223530 A	13-08-1992
			US 5249294 A	28-09-1993
EP 0463855	A	02-01-1992	JP 4054652 A	21-02-1992
			US 5751988 A	12-05-1998
EP 0417817	A	20-03-1991	AU 631246 B	19-11-1992
			AU 6261690 A	21-03-1991
			CA 2025518 A	16-03-1991
			US 5220661 A	15-06-1993

PCT

**AVIS INFORMANT LE DEPOSANT DE LA
COMMUNICATION DE LA DEMANDE
INTERNATIONALE AUX OFFICES DESIGNES**

(règle 47.1.c), première phrase, du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

CORLU, Bernard
Bull S.A.
PC59C18
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 07 janvier 1999 (07.01.99)		
Référence du dossier du déposant ou du mandataire PCT 3630/BC		AVIS IMPORTANT
Demande internationale no PCT/FR98/01343	Date du dépôt international (jour/mois/année) 25 juin 1998 (25.06.98)	Date de priorité (jour/mois/année) 26 juin 1997 (26.06.97)
Déposant BULL CP8 etc		

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:

CN,EP,JP,KR,US

Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:

Aucun

La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le 07 janvier 1999 (07.01.99) sous le numéro WO 99/00718

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, la demande d'examen préliminaire international doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse	Fonctionnaire autorisé J. Zahra
no de télécopieur (41-22) 740.14.35	no de téléphone (41-22) 338.83.38